This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for a processor of a computing device to obtain a trusted identification of a hardware peripheral of the computing device, the processor and the peripheral being coupled by a path through which data is to be exchanged therebetween, the method comprising:

the processor and the peripheral deriving a set of shared keys based on the identification of the peripheral by:

the processor and the peripheral each generating a random value, performing a first operation based on the random value thereof to produce an intermediary value, and sending the produced intermediary value to the other by way of the path;

the peripheral generating a signed representation of the intermediary value and sending the signed representation to the processor by way of the path, the signed representation being verifiable by the processor according to the identification of the peripheral;

the processor and the peripheral each performing a second operation based on the intermediary value from the other and also based on the random value thereof to produce a final value, the final value as produced by the processor being equal to the final value as produced by the peripheral and thus constituting a shared secret known only to the processor and the peripheral;

the processor and the peripheral each employing the shared secret to generate the set of shared keys;

the processor requesting by way of a trusted hardware channel that the peripheral provide the identification to such processor by way of such trusted channel, the trusted channel being independent of and exterior to the path;

the processor receiving by way of the trusted hardware channel the identification from the peripheral; and

the processor, having prior knowledge of the peripheral and the identification thereof, concluding based on the received identification by way of the trusted channel that the

peripheral is indeed the peripheral and imparting trust to the peripheral based on such conclusion, and exchanging data with the peripheral over the path based on the identification.

2. (Currently Amended) The method of claim 1 further comprising ~~the processor~~ the processor and the peripheral employing the identification to derive a set of mutually agreed-upon shared keys to be employed to exchange data therebetween, and in fact exchanging data therebetween based on the ~~derived~~ set of mutually agreed-upon shared keys.

3. (Original) The method of claim 1 wherein the computing device includes a trusted hardware module (THM) physically interposed between the processor and the peripheral to form the trusted hardware channel therebetween, the THM being trusted to communicate with both the processor and the peripheral in a trusted manner over the trusted channel and being identifiable to the processor over the trusted channel, the method comprising:

the processor requesting the THM over the trusted channel formed thereby to obtain the identification from the peripheral;

the THM in turn requesting the peripheral over the trusted channel formed thereby to provide such identification;

the peripheral returning the identification to the THM over the trusted channel formed thereby; and

the THM in turn returning the identification to the processor over the trusted channel formed thereby,

whereby each request and return over the trusted channel assures the processor that the identification returned is in fact from the peripheral.

4. (Original) The method of claim 3 wherein the peripheral includes therewith a unique public-private security key pair (PU-PER, PR-PER), and wherein the identification of the peripheral is (PU-PER).

5. (Original) The method of claim 1 wherein the peripheral includes therewith a unique public-private security key pair (PU-PER, PR-PER), and wherein the identification of the peripheral is (PU-PER).

6. (Cancelled)

7. (Original) A method for a processor of a computing device and a hardware peripheral of the computing device to derive a set of shared keys, the processor and the peripheral being coupled by a path through which data is to be exchanged therebetween, the method comprising:

the processor and the peripheral each generating a random value, performing a first operation based on the random value thereof to produce an intermediary value, and sending the produced intermediary value to the other by way of the path;

the peripheral generating a signed representation of the intermediary value and sending the signed representation to the processor by way of the path, the signed representation being verifiable by the processor;

the processor and the peripheral each performing a second operation based on the intermediary value from the other and also based on the random value thereof to produce a final value, the final value as produced by the processor being equal to the final value as produced by the peripheral and thus constituting a shared secret known only to the processor and the peripheral; and

the processor and the peripheral each employing the shared secret to generate the set of shared keys.

8. (Original) The method of claim 7 further comprising the processor obtaining a trusted identification of the peripheral, and comprising the processor verifying the signed representation according to the obtained trusted identification.

9. (Original) The method of claim 7 comprising the processor and the peripheral forming a Diffie-Hellman key exchange to produce the shared secret.

10. (Original) The method of claim 7 comprising the processor and the peripheral each employing the shared secret to generate a shared symmetric content key KC to encrypt and

decrypt data sent between the processor and the peripheral and a shared symmetric MAC key KM employed as part of a MAC algorithm to sign sent data and verify same.

11. (Original) The method of claim 10 wherein the processor and the peripheral each calculate KC and KM from the shared secret z based on a pre-determined one-way hash function HASH and based on common access to commonly known constants K1 and K2, where:

$$KC = HASH (K1, z), \text{ and}$$
$$KM = HASH (K2, z).$$

12. (Original) The method of claim 7 wherein the processor and the peripheral mutually generate based on the shared secret a shared symmetric content key KC to encrypt and decrypt the data and a shared symmetric MAC key KM employed as part of a MAC algorithm to sign the data and verify same, the method further comprising the processor sending trusted data to the peripheral by:

the processor retrieving the data from a trusted section of a memory of the computing device, encrypting such data according to the content key KC, performing the MAC algorithm over the encrypted trusted data according to the MAC key KM to produce MAC data, storing the encrypted trusted data in a non-trusted section of the memory, and storing the MAC data in such non-trusted section of the memory;

the processor storing information regarding how to access such stored encrypted trusted data and MAC data in the memory as a transfer descriptor in the non-trusted section of the memory, and then providing the peripheral by way of the path with a physical address of such transfer descriptor in such memory;

the peripheral accessing the transfer descriptor in the memory at the physical address thereof by way of the path, reviewing the information in the transfer descriptor, and retrieving the stored encrypted trusted data and MAC data in the memory based on the information and by way of the path, and

the peripheral verifying the retrieved encrypted trusted data based on the retrieved corresponding MAC data and according to the MAC key KM, and presuming such

verification succeeds, the peripheral decrypting the retrieved encrypted trusted data based on the content key KC and rendering the decrypted trusted data.

13. (Original) A method for a processor of a computing device to send trusted data to a hardware peripheral of the computing device, the processor and the peripheral being coupled by a path through which the data is to be exchanged therebetween, the method comprising:

the processor and the peripheral mutually generating a shared symmetric content key KC to encrypt and decrypt the data and a shared symmetric MAC key KM employed as part of a MAC algorithm to sign the data and verify same;

the processor retrieving the data from a trusted section of a memory of the computing device, encrypting such data according to the content key KC, performing the MAC algorithm over the encrypted trusted data according to the MAC key KM to produce MAC data, storing the encrypted trusted data in a non-trusted section of the memory, and storing the MAC data in such non-trusted section of the memory;

the processor storing information regarding how to access such stored encrypted trusted data and MAC data in the memory as a transfer descriptor in the non-trusted section of the memory, and then providing the peripheral by way of the path with a physical address of such transfer descriptor in such memory;

the peripheral accessing the transfer descriptor in the memory at the physical address thereof by way of the path, reviewing the information in the transfer descriptor, and retrieving the stored encrypted trusted data and MAC data in the memory based on the information and by way of the path, and

the peripheral verifying the retrieved encrypted trusted data based on the retrieved corresponding MAC data and according to the MAC key KM, and presuming such verification succeeds, the peripheral decrypting the retrieved encrypted trusted data based on the content key KC and rendering the decrypted trusted data.

14. (Original) The method of claim 13 comprising the processor storing information regarding how to access such stored encrypted trusted data and MAC data in the memory as a transfer descriptor in the non-trusted section of the memory, the transfer descriptor including a contiguous array of ordered entries, each entry describing a block or series of contiguous

blocks of data in the memory, including a physical address and length, whereby the encrypted trusted data and the MAC data are reconstructed according to such ordered entries.

15. (Original) The method of claim 13 comprising the processor and the peripheral mutually generating KC and KM based on a shared secret.